Department of the Navy
Naval Information Systems
Management Center

NAVSO P-5239-01
May 1995

INTRODUCTION TO

INFORMATION SYSTEMS SECURITY

(INFOSEC)

GUIDEBOOK

MODULE 01

INFORMATION SYSTEMS SECURITY
(INFOSEC)
PROGRAM GUIDELINES

0515-LP-208-8200

Distribution: Submit requests for placement on distribution (including supporting justification), or amendment to the existing distribution, to:

Commanding Officer
Naval Command, Control and Ocean Surveillance Center
ISE East Coast Division
Code 422
3801 Nebraska Avenue, N.W.
Washington, DC 20393-5270

Commercial (202) 764-0753
DSN 764-0753
E-Mail: subscribe@infosec.nosc.mil

Electronic versions of this document may be download via anonymous ftp from infosec.nosc.mil or //http://infosec.nosc.mil/inf.html.

Stocked: Additional copies of NAVSO P-523 9-15 can be obtained from the Navy Aviation Supply Office (Code 03415), 5801 Tabor Avenue, Philadelphia PA 18120-5099, through normal supply channels in accordance with NPFC PUB 2002D, NAVSUP P-437 or NAVSUP P-485, using AUTODIN, DAMES, or MILSTRIP message format to DAAS, Dayton, OH.

Cite stock number 0515-LP-208-8200.

DEPARTMENT OF THE NAVY

NAVAL INFORMATION SYSTEMS MANAGEMENT CENTER
WASHINGTON, D.C. 20360-5000

NAVSO P-5239-01

MAY 1995

FOREWORD

Navy Staff Office Publication (NAVSO Pub) 5239, "Information Systems Security (INFOSEC) Program Guidelines" is issued by the Naval Information Systems Management Center. It consists of a series of modules providing procedural, technical, administrative and/or supplemental guidance for all information systems, whether business or tactical, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or receipt of data. Each module will focus on a distinct program element and describe a standard methodology for planning, implementing and executing that element of the INFOSEC program within the Department of the Navy (DON).

This module, "Introduction to Information Systems Security (INFOSEC) Guidebook", provides a basic introduction to INFOSEC and summarizes the DoN INFOSEC Program.

The guidance contained herein applies to all DON AIS's and is effective upon receipt.

J. G. HEKMAN
Rear Admiral, SC, USN

TABLE OF CONTENTS

1.0 INTRODUCTION

This module introduces the Naval Staff Office Publication (NAVSO P) 5239 series. This series provides Information Systems Security (INFOSEC) guidelines, procedures, and processes to help the Department of the Navy (DON) meet INFOSEC security requirements.

1.1 Scope and Purpose

For NAVSO P 5239 Series

The NAVSO P 5239 series is composed of a series of modules, each providing guidance and information on a specific area of INFOSEC. Several of the modules are targeted at specific INFOSEC communities. Other modules of the NAVSO P 5239 series are geared toward a more general audience, providing information and guidance appropriate to DON information system managers and users. Altogether, the NAVSO P 5239 series provides a set of sources and guidebooks that assist in planning and operating information systems and help system users maintain security awareness. Appendix A provides a complete list of the NAVSO P 5239 modules.

For Module One

This module introduces and summarizes the Navy's approach to INFOSEC. It applies to information systems processing unclassified, sensitive but unclassified and classified information. By using this information, system planners and organizational managers (e.g., Designated Approval Authorities [DAAs], Information System Security Officers [ISSOs], Information Systems SecurityManagers [ISSMs]) and users (e.g., system administrators and end users) will have a common understanding of INFOSEC principles, concepts, and interrelationships.

1.2 INFOSEC Definition

INFOSEC is defined in the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009. The NSTISSI 4009 definition, paraphrased, is: the protection of information systems against (1) unauthorized access to or modification of information, (2) denial of service to authorized users and (3) provision of service to unauthorized users. INFOSEC also includes the measures necessary to detect, document, and counter those threats.

COMPUSEC + COMSEC + TEMPEST = INFOSEC

Previously, separate security policies and doctrines addressed protection of computer systems (COMPUSEC), information transfer systems (i.e., communications security [COMSEC]), and compromising emanations (TEMPEST). With today's growth of information processing networks and weapon systems with information processing capabilities, the separate implementation of these related disciplines for information protection is no longer technically or fiscally feasible.

INFOSEC is the current discipline that provides an integrated and systematic approach to the security of all aspects of information systems through their life cycles. The term "information system" is used throughout this document to mean any system that processes, stores or transfers data or information.

1.3 INFOSEC Overview

The DON has determined that all DON information systems are sensitive regardless of whether the information is classified or unclassified. This means that all DON information systems must provide some combination of confidentiality, integrity, and availability protection mechanisms in accordance with Public Law 100-235. To this end information systems must employ features to ensure that only authorized users who require access may access the data and that the data is valid.

DON information systems process, store, and transfer large quantities of information. This information is critical to the naval war fighting and support missions. Internetworking of information systems has expanded rapidly in the last decade and has resulted in newly integrated distributed networks with multiple, worldwide uses. The information flow among these systems will continue to expand rapidly as systems are further integrated under the Global Command and Control System (GCCS) architecture and connected via the National Information Infrastructure (NII) and the Defense Information Infrastructure (DII) backbones.

The expected outcome of these information system advances is universal access to any

TABLE 1
INFOSEC SYSTEMIC THREATS

Threats/ Resources	Browsing	Misuse	Penetra-tion	System Flaws	Component Failure	Tampering	Eaves-dropping	Message Stream Modification	Denial of Comms	Traffic Flow Analysis
Information	•	•	•	•	•	•				
Hardware		•		•	•	•				
Software	•	•	•	•	•	•				
Telecom-munications		•			•	•	•	•	•	•
Personnel*		•								
Documen-tation	•	•								

* For the purposes of this table, personnel are considered a resource of the system and , thus, they require protection and are not a threat to the system.

information, as permitted by security access controls. These advances in information system capabilities and information flow have also increased the vulnerability of naval information systems to exploitation by both accidental exposure and malicious threat agents. Current information systems may be vulnerable to any or all of the threats shown in Table 1.

The INFOSEC challenge, to protect information in this new environment, has required a significant reorientation from traditional, stand-alone COMSEC and COMPUSEC approaches. The traditional, stand-alone, box-oriented approaches are being replaced with a fully integrated system security approach (i.e. INFOSEC) that combines COMPUSEC and COMSEC. The focus of the DON INFOSEC program is to provide sufficient security to reduce risk to information system assets to acceptable levels.

2.0 DoN INFOSEC PROGRAM

The DON INFOSEC program is designed to comply with the national, Department of Defense, and DON INFOSEC policies. A synopsis of the significant directives, regulations, instructions, and public laws is included as Appendix B. These policies stipulate that security must be considered throughout the life cycle of information systems. Requirements derived from these policies guide the development of products, techniques, and capabilities to satisfy the DON INFOSEC objectives and to promote the implementation of innovative information systems technology. The DON INFOSEC program has two objectives:

- Provide a complete set of services to information system developers and users by planning, developing, acquiring, implementing, fielding, and supporting critical INFOSEC products, techniques, and designs.

- Provide systems security engineering and integration of critical INFOSEC products, techniques, and designs into DoN information systems .

The DON INFOSEC program is targeted for two major audiences:

- The operational user: By identifying INFOSEC needs, upgrading or implementing security in existing information systems, and providing security awareness and training.

- The DON Program Managers (PM): Assists the PM in developing and fielding information systems (including weapons systems) by identifying security requirements and by providing INFOSEC engineering support and products.

3.0 DON INFOSEC PROGRAM COMPONENTS

The DON INFOSEC program is a fully integrated system security approach that helps reduce security risk in information systems. Its success depends on how well:

- Information planners and organizational managers analyze, derive, and reduce the risks resulting from the threats that target information systems.
- DON information system sponsors, developers, and users understand and maintain an adequate level of security awareness.
- The commands responsible for developing and incrementally upgrading information systems understand the components that constitute the DON integrated INFOSEC approach.

Those components include:

- *DON Systems Resources,* which include all the resources that support a system's ability to control, process, store, and transfer information. These resources need to be reviewed for targeted threats/potential threats.
- *INFOSEC Functionality,* which includes the assurances that the system sponsor, designer, and user expect to achieve through the use of INFOSEC measures. INFOSEC functionality includes *confidentiality, integrity, and availability*.
- *Threats and Risk,* which are the primary reasons for applying INFOSEC solutions to DON. The threats which may exploit a system's vulnerabilities (security weaknesses) or threats that subsequently make a system vulnerable need to be assessed to determine how INFOSEC can reduce risk s to DON Systems.
- *INFOSEC Measures,* which include Technology, Policies and Procedures, and Education and Awareness measures that can be applied in a variety of combinations to help reduce risk.

3.1 DON Systems Resources

The DON INFOSEC program is driven by a need to reduce risk to system resources by identifying their vulnerabilities to specific threats and applying INFOSEC measures to prevent the likelihood or reduce the impact on system assets from a threat occurrence. In reviewing a system’s INFOSEC posture, the following resources should be considered:

- Information
- Hardware
- Software (including Firmware)
- Telecommunications
- Personnel
- Documentation.

These resources collectively allow a system to process , store, and transfer information and affect its INFOSEC posture. To define potential risk areas, each security function should be considered in relationship to the system's operational mission, threats, and components.

3.1.1 Information

The purpose of INFOSEC is to ensure that information is protected from unauthorized disclosure or modification and is available when needed. Information in a system exists in one of three states: processing, storage, and transfer. Information in the processing state is being manipulated by the information system. Information in the storage state is being maintained by the information system on storage devices such as a disk, tape, CD-ROM or programmable read-only memory (PROM). Information in the transmission state is being sent from one component to another. These components could be processors, networks, or auxiliary devices such as printers and storage devices. The goal of the Navy INFOSEC program is to protect information regardless of its state. System availability is not solely an INFOSEC concern and INFOSEC is not responsible for all aspects of system availability.

3.1.2 Hardware

To protect the information being processed, stored, or transferred by an information system, it is necessary to protect the hardware performing these functions. If unauthorized persons are able to gain access to the hardware, such as the central process ing unit (CPU) or disk drives (internal or floppy disks), they could make unauthorized changes that might cause the hardware to:

- Allow unauthorized disclosure of the information by writing the information to another file that could later be retrieved

- Allow unauthorized modification of the information that would send incorrect information to a recipient

- Create a denial-of-service situation that would prevent authorized users from gaining access to the information required to perform their duties.

3.1.3 Software

A system's software (including firmware) must be protected to ensure the integrity of the information being processed, stored, or transferred. Software needs to be protected during development, while it is being transferred to the system, and during operational use.

- Development – To ensure unintentional errors or malicious software is not introduced during software development and to ensure adequate protective features are engineered into the design to protect system software and data during product operations.

- Transfer – To ensure that software sent from a programming facility (e.g., a software support facility or a contractor's plant) arrives at the system unchanged

- Operational Use – To ensure unintentional errors or malicious software is not introduced into the system.

Software that needs to be protected includes operating systems, system utilities, and application programs. Essentially, any software that has the ability to access the information must be protected to ensure that it performs only authorized actions on the information. Any unauthorized changes to the software could have the same results as those caused by changes to the hardware described in the preceding section. Attempting to ensure that no unintentional errors occur during software development is not solely an INFOSEC issue, nor is INFOSEC solely responsible.

3.1.4 Telecommunications

For an information system to be of any value, users need to be able to communicate with the system and transfer information to other users and other systems without the communication path itself facilitating unauthorized access to the system. The user's workstation may connect directly to a system through a modem, or via a network (either local or wide area). Regardless of the specific mechanism used to communicate with the information system, it is essential that the user be assured that information can be transmitted when required and with confidentiality and data integrity ensured.

3.1.5 Personnel

Personnel are critical to the correct operation of information systems. System and security administrators ensure that the system is configured and working properly. Users both receive the system information and use the system to perform their duties. User error or improper use or intentional misuse of the system by any of the personnel may result in a degradation of the information or the system itself. All of the personnel working with the system must be trained in system operations and aware of general security threats to ensure effective and secure use of the system and its information. All personnel working with the

system must have the right level of clearances and the need-to-know to process the information.

3.1.6 Documentation

Documentation that describes the hardware and software of the information system is critical to its proper operation and maintenance. Documentation supporting the hardware and software is necessary to:

- Describe the system's security features
- Maintain the system in its current operational state
- Recreate the system in the event critical assets are destroyed and an alternate measure must be used
- Describe the risk associated with operating the system and plan improvements to the system, including security improvements, as technology permits.

3.2 CRITICAL INFOSEC INFORMATION CHARACTERISTICS

A component of DON information systems is the set of in-place countermeasures that provide INFOSEC features. This section discusses the three primary INFOSEC functional areas (confidentiality, integrity, and availability). These three functional areas need to be considered to ensure that adequate countermeasures are employed to meet and counteract the identified and potential threats.

3.2.1 Confidentiality

Confidentiality is the protection of information from disclosure to unauthorized parties. It is often the most critical security function for an information system. It may also limit access to sensitive data to an appropriate set of individuals or organizations. It is concerned with information where the disclosure would be undesirable or unlawful and is not limited to the protection of sensitive user information, but also includes protection of management functions. For example, system administrator functions of a network should be protected from general users. Confidentiality is typically implemented using several types of protection, including cryptography and access controls.

Access control helps ensure that users have access to only the information and functions for which they are authorized. Two forms of access control may be implemented.

- Mandatory access controls ensure that critical control requirements (for example, classification restrictions) are enforced.

- Discretionary access controls ensure that need-to-know or compartmentalization requirements are enforced.

Access control mechanisms may include simple protections (e.g., passwords) and assignment of specific system permissions to a limited set of personnel (for example, LAN administrators). Access controls may also ensure that only the tools and information necessary to accomplish a task can be accessed and that other system tools and information are protected.

3.2.2 Integrity

Integrity is the assurance that information processed, stored, or transferred within a system will not be accidentally or maliciously manipulated, altered, or corrupted. Additionally, integrity functionality supports the ability to detect information that has been altered, unintentionally or maliciously. Mechanisms implementing the integrity function may include :

- Time and date stamping to ensure that the order of data is not altered or that data recorded by an adversary is not replayed at a later time to "spoof" the system

- Checksums or digital signatures to protect the exchange of data between systems and components

- Message attributes like length, message type, headers, format, content, addressing, or precedence to verify message integrity.

Software integrity security functions may also be used to protect software from undetected and unauthorized modification, manipulation, and destruction. As with data, the software may also have checksums or other integrity validation methods instituted to verify its integrity.

Nonrepudiation may be considered a subset of integrity. There are two categories of nonrepudiation: origin and destination. Origin n onrepudiation provides the recipient with proof of the origin of the information. Destination nonrepudiation provides the sender with proof of delivery. Origin and destination nonrepudiation protect against attempts by the sender to deny sending information and attempts by the recipient to deny receiving the information.

3.2.3 Availability

Availability supports the accessibility and reliability of the system and provides assurance of continuity of operations. Availability-focused countermeasures protect against degraded capabilities and denial of service conditions. Availability countermeasures address

general operational capabilities and specific operational standards. As an INFOSEC characteristic availability addresses malicious attempts to degrade system operations

Security mechanisms that help to ensure availability include:

- Duplication of critical system functions
- Security audit and alarm procedures
- System resource usage controls
- Robust routing algorithms

3.3 Threats and Risks

The system security determination is based on the vulnerabilities, threats, countermeasures, and risks that can be identified for an information system.

- A vulnerability is a weakness in a system that can be exploited.
- A threat is a circumstance or event that exploits a given vulnerability.
- Countermeasures are mechanisms designed into an information system to reduce its vulnerabilities.
- Risk is the probability that a given threat will exploit a given vulnerability and the existing countermeasures will not stop the threat.

A risk assessment is performed to evaluate system assets and potential threats and associated vulnerabilities that may impact these assets and to determine the risk status of a system after the implementation of countermeasures. A determination of an acceptable level of risk is essential in deciding that a system may be used operationally. This section discusses the relationship between threats and risks and provides examples of each.

3.3.1 Threats

Threats are those circumstances with the potential to disrupt the confidentiality, integrity, or availability properties of a system. Some prominent systemic threats are:

- Browsing
- Misuse
- Penetration
- System Flaws

- Component Failure
- Tampering
- Eavesdropping
- Denial of Telecommunications
- Traffic Flow Analysis.

Each of these threats is discussed below. These examples do not include "nonhostile" threats such as flood, fire, loss of power, or poor communications media. However, a complete INFOSEC system analysis and implementation will address both adversarial and nonhostile threats.

Browsing threats are attempts by a user or intruder to access information for which read access is not authorized or intended. Browsing includes the threat of unauthorized personnel:

- Gaining access to sensitive information
- Reading information left on a terminal screen
- Reading the hard copy outputs
- Accessing system files or other user files
- Accessing the information written into and read out of system memory.

Browsing could violate need-to-know requirements or clearance authorizations and result in the unauthorized disclosure of sensitive or classified information .

Misuse threats are the use of processing or communication services for other than official or authorized purposes. Misuse includes:

- Execution of malicious functions either inadvertently or intentionally
- Perpetration of errors of commission, omission , or oversight
- Introduction of malicious software (e.g., computer viruses or Trojan horses) into the system
- Modification of data either maliciously or inadvertently
- Monopolization of system resources , making them inaccessible to other users or devices in the system
- Transmission of information without the proper system permissions
- Observation of keystrokes of authorized personnel to gain s ystem information (e.g., password entry and protected function commands).

Misuse could result in unauthorized disclosure or modification of information, receipt of services by unauthorized personnel, or denial of service to legitimate users.

Penetration threats involve attacks by unauthorized persons attempting to gain system access by defeating the system security perimeter. Penetration is often carried out with browsing or misuse, and could result in:

- Unauthorized disclosure or modification of information
- Receipt of services by unauthorized personnel
- Denial of service to legitimate users.

Penetration threats typically involve system login or access control mechanisms where an unauthorized person has the ability to bypass or subvert the login mechanism or has access to system functions or information for which permissions have not been granted.

System flaws are threats that involve both intentional and unintentional errors in the system hardware and software that result in undesirable events. System flaws result from poor engineering practices or the malicious introduction of errors. System flaws in security mechanisms can result in the violation of the system security policy through unauthorized disclosure or modification of information and unauthorized receipt of services.

Component failure threats involve malfunctions in the system hardware, software, or media. Component failure could be the result of faulty equipment, unanticipated system events, or environmental effects, and could result in denial of service conditions. Failure of components that implement security mechanisms could result in the violation of the system security policy through unauthorized disclosure or modification of information, unauthorized receipt of services, or denial of service to legitimate users.

Tampering threats involve attacks to physical and logical components of the system. Tampering attacks may include:

- Substituting rogue components for legitimate components to intercept communications, generate incorrect or misleading information, masquerade as a legitimate component, or perform other undesirable functions
- Stealing components
- Damaging components to destroy or render them useless
- Electrical probing within the system to reveal sensitive information or to explore the details of sensitive technology.

Tampering may be committed throughout a system, and could result in unauthorized disclosure or modification of information, unauthorized receipt of services, or denial of service to legitimate users.

Eavesdropping threats involve passive surveillance of telecommunication channels to illicitly gain access to information transferred over those assets. Eavesdropping may be done through physical, electrical, and radio-frequency taps into the telecommunication channel or system device emanations. It could result in the unauthorized disclosure of information transferred over telecommunication channels. Eavesdropping includes:

- Electrical tapping of wirelines to gain useful system infor mation
- Overhearing conversations that could provide useful information to a malicious user
- Detecting and intercepting radio or electrical-magnetic signals
- Network sniffers
- Redirecting or rerouting messages/information

Message stream modification threats involve attempts to modify, delete, reorder, duplicate, insert, or create information while it is being transferred over a communication channel. Message stream modification attacks may be done at any point in the communication architecture. Modification threats include:

- Deleting or reordering information in the message stream
- Replaying message stream information that was previously recorded
- Causing the system to transfer data in error
- Causing an error to occur during transmission.

Denial of telecommunication threats involve preventing or delaying the performance of telecommunication services. As with message stream modification attacks, denial of telecommunication attacks may be done at any point in the telecommunication architecture. Denial of telecommunication threats include:

- Electrical jamming
- Radio frequency jamming
- Failure of equipment or the destruction of the transferred message caused by the electromagnetic wave resulting from a nuclear explosion or similar electromagnetic event
- Traffic flooding in which traffic flow becomes too great for the system to handle
- Misuse or misallocation of telecommunication resources.

- Redirecting of messages

Traffic flow analysis threats involve the passive collection, analysis, and interpretation of telecommunication patterns to gain operational- and logistics-related information. Traffic flow analysis may be done using the same techniques as eavesdropping and could result in the unauthorized disclosure of sensitive operations or logistics information. Traffic flow analysis includes:

- Analysis of the telecommunication characteristics of a certain transmitter
- Tracking of a transmission facility through the interception of signals
- Analysis of message transmission patterns and data to gain information about transmission capabilities and possible message destinations .

Covert channel analysis determines the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to the information. Covert channel analysis includes all forms of covert channels, external as well as internal, and timing as well as storage channels.

3.3.2 Risks

Risk is a measure of the potential for loss from a system. It is a combination of system vulnerabilities, of the likelihood that a threat will exploit a given vulnerability, and of the likelihood that the exploitation attempt will not be stopped by system countermeasures. Risk also includes an analysis of the likelihood that a threat occurrence will result in an adverse impact and assesses the severity of the adverse impact. Determining that the measured risk for an information system is acceptable is the final factor in determining if a system may be used operationally. A risk determination is required because it is nearly impossible to completely correct all vulnerabilities associated with an information system. The risk assessment will determine what the vulnerabilities are, determine the likelihood that threats will exploit a given vulnerability, and predict the potential impact to the system if the vulnerability is exploited. Given all the factors in the risk equation and the cost of implementing some countermeasures, a determination may be made that the risk potential of a given vulnerability is not worth the cost of correcting or implementing a countermeasure.

Consider two workstations exchanging data between two buildings via cabling through a courtyard. The data they are exchanging is unclassified but sensitive (e.g., personnel information). Because the data is sensitive, a security policy for this system might include confidentiality and integrity; but because it is administrative, availability may not be considered critical. The most prominent vulnerability in the system is the unprotected telecommunications link through the courtyards. Consequently, threats of eavesdropping and

message modification exist. Several countermeasures could be used to reduce these threats. The cable could be buried, placed in conduit and concrete, be rerouted through a protected space, or the data could be encrypted. The amount of residual risk would be dependent on which of the protection methods was used and whether a threat was likely to occur and the potential impact of its occurrence. If the data is sensitive but not classified, it may be determined that the risk is acceptable with no additional protection. If the data is classified, protection of the cable and encryption may be required to reach an acceptable level of risk.

3.4 INFOSEC Security Measures

To mitigate the risks associated with operating an information system and to ensure the confidentiality, integrity, and availability of information and those system resources that support that information (as described in Section 3.1), security measures need to be implemented. These security measures fall into three broad categories:

- Technology (e.g., design of hardware and software configurations and cryptographic equipment)
- Policies and procedures (e.g., policy/guidance on the use of a system, standard operating procedures, security operating procedures and incident reporting and control procedures)
- Education, training, and awareness (e.g., system security education, threat awareness, and proper system operations training).

By using a combination of the measures in these three categories, the security of the information in a system and the security of the system itself can be maintained.

3.4.1 INFOSEC Technology Measures

Technology can be implemented in hardware or software components. A technology measure could be as simple as a user ID and password used by the operating system or as complex as a smart card used for identification and authentication of a user. Typically, technology measures are thought of as supporting the following security disciplines:

- COMPUSEC (identification and authentication, access controls, and auditing)
- COMSEC (cryptographic devices)
- TEMPEST (emanations protection).

3.4.2 INFOSEC Policy and Procedures Measures

Policy and procedures are also vital INFOSEC measures. A strong, enforced security policy provides the basis for all system security. Likewise, strong procedures that are followed complement the technology and training and awareness measures. Procedures help to ensure that the technology is used correctly. Procedures can also ensure that security mechanisms not addressed by technology are addressed through other measures. For example, procedures may be in place to ensure that only authorized personnel have physical access to a workstation connected to an information system. Other procedural measures may include the requirement for alphanumeric passwords of a minimum size and frequent password changes.

3.4.3 INFOSEC Training and Awareness Measures

Policy and procedure measures are not likely to be effective if involved personnel do not know they exist or how they are used. Training and awareness measures must be in place so that all information system users know the technology measures in place and the policies and procedures that must be followed. Effective training and awareness measures will ensure that all personnel associated with the use, maintenance, and operation of an information system are aware of the technical and procedural security measures that are in place to protect the information. System administrators need to be trained to configure the system and options correctly so that the information and system resources are provided the necessary protection. Users need to be trained in the correct usage of the security measures.

Additionally, an awareness program helps to ensure that all personnel associated with the use, maintenance, and operation of an information system are aware of the threats that are applicable to the system and the measures required to mitigate the threats. An awareness program can be one method to ensure that INFOSEC policy and procedures are understood by all personnel who work with the information system.

4.0 SECURITY ASSURANCE ACTIVITIES

Section 3 discussed the process of applying INFOSEC to an information system through consideration of system resources, INFOSEC functionality, threats and risks, and INFOSEC measures. The final step in placing an information system into operation is to apply standard methods to ensure that risks to the system are reduced to known and acceptable levels, and that these risks can be reviewed and reassessed in the future. The primary method to measure residual risk to a system and determine its INFOSEC posture and operational suitability is the certification and accreditation process.

4.1 Certification

Certification is the technical evaluation of a system ’s security features and is performed as part of the accreditation process. It establishes the extent to which a system’s design and implementation of security features satisfy the security requirements. Certification

activities include reviewing design documentation, performing risk assessments, and conducting certification tests. Certification testing is conducted by both the developer and the Government. After certification testing is successfully completed, the certification authority will certify the system. The certification decision is based on a review of the system design documentation, the risk assessment(s), and the review and interpretation of the certification test results. The certification authority will issue a certification statement that documents the extent to which the system meets its security requirements.

4.2 Accreditation

After the system has been certified, but before it can be placed into operation, it must be evaluated in its operational environment and the risks associated with operating the system assessed. A DAA is assigned to review the certification package, assess the risks of operating the system in its operational environment, and accredit the system for operation. Accreditation may include security test and evaluation (ST&E) activities whe n the system is operationally tested by users to determine the security posture of the system.

Upon completion of the accreditation process, the DAA may take one of the following four actions:

- Accredit the system to process information in the given operational environment.
- Issue an Interim Authority To Operate (IATO). An IATO is issued when the DAA determines that changes must be made to the system or its environment, but the system will be allowed to operate in the interim. An IATO may not exceed one year.
- Reject accreditation and recommend enhancements that will lead to accreditation.
- Reject accreditation because of inherent security deficiencies and provide rationale.

Accreditations are valid for up to 3 years unless there is some major change to the system configuration. Accreditation must also be reviewed when changes are made to system functionality, architecture, interfaces, information processed, environment, and user communities because these changes may increase the risk to the system.

5.0 RELATIONSHIPS AND RESPONSIBILITIES

The DON INFOSEC program was established to ensure that each Naval information system has mechanisms to protect the information processed by that system. To ensure that this program is implemented at each DON activity and for each DON information system, several roles with associated security responsibilities have been established through which DON program managers translate user INFOSEC requirements into information systems. Within each activity, the Designated Approving Authority (DAA) and the Information Systems Security Manager (ISSM) are the cornerstone of the activity's implementation of the DON INFOSEC Program.

The DAA is the management official who makes the decision that an information system can be operated with the known level of risk by accepting responsibility for that risk. Typically, this management official is the commanding officer or a senior officer of the activity, but there are some exceptions. The accreditation decision of the DAA is based on the operational need for and the threats to the system. The DAA must make an accreditation decision based on a trade-off between the operational need for and the criticality of the system (and its information) against the risks the known threats pose.

The ISSM is the DAA's technical security advisor. The DAA will rely on this person to establish and maintain the security of the information system. For small activities with only a few systems, one person may serve as the ISSM for all the systems within the activity. For larger activities with many systems, there may be several ISSOs, one for each system or group of systems coordinated and managed by the ISSM.

Larger systems may also have Terminal Area Security Officers (TASOs) who assist the ISSOs in the performance of their duties. Typically, the TASOs are responsible for specific terminal, office, or work areas that are connected to the system. The ISSOs are responsible for ensuring that the appropriate technical and procedural measures are established for their systems. These measures include a training and awareness program, access control to the hardware, software, and data, auditing of user actions, a risk management program, and an adequate contingency plan.

Appendix A

Planned Naval Staff Office Publication 5239 Modules (Note: the modules are not listed in publication order. Asterisked modules have been published. All others are planned.)

5239-01 Introduction to Information Systems Security (INFOSEC)

Provides a basic introduction to INFOSEC and summaries the DoN INFOSEC Program.

5239-02 Terms, Abbreviations, and Acronyms

Lists and defines INFOSEC terms, acronyms, and abbreviations that have been standardized for use within the DoN.

5239-03 Designated Approving Authority Guidebook

Provides guidance to the DAA in focusing the efforts of the activity security staff. Contains synopsis of certification and accreditation process. Offers the DAA a step-by-step approach to assist in reaching accreditation decisions.

5239-04 Information Systems Security Manager Guidebook

Provides guidance to the individual assigned responsibility for INFOSEC implementation and operation at Navy activities. Additional TEMPEST guidance is provided for ISSMs at SYSCOMs, CINCs, and other echelon II commands. Illustrates the need for management involvement and support for the security program.

5239-07 Information Systems Security Officer's Guidebook

Aids those who carry out and administer INFOSEC programs for specific AISs and LANs. Helps ISSOs understand the requirements, identify the necessary planning, and conduct an effective INFOSEC program.

5239-08 Network Security Officer's Guidebook

Provides policy and step-by-step procedures to individuals responsible for accomplishing a risk analysis on WANs. Provides methods for the determination of system sensitivity and criticality, accomplishment of risk assessment and economic analysis, and determination of environmental hazards and threats to DoN information systems.

5239-10* **Assessed Product List**

Identifies products which have been evaluated for features and assurance of trust.

5239-11 **System Security Requirements Development**

Provides guidance on how to develop a security policy and security requirements for a specific system.

5239-12 **Acquisition Life Cycle Guidebook (PMs/Developers)**

Identifies key technical and management actions need from Program Managers and other developers who have managerial and technical responsibilities for acquiring or certifying computer systems. Oriented primarily towards Program Managers, it focuses on the processes and requirements needed to certify and accredit information systems.

5239-13 **Certification & Accreditation Guidebook**

Provides procedural guidance and decision aids for conducting C&A process activities to determine the suitability of a system to operate in a targeted operational environment based on the degree of assurance required and other factors related to a system.

5239-14 **Security Architecture Guidebook**

Serves as a compendium of proven solutions to DON INFOSEC problems to assist INFOSEC systems engineering and customer support professionals to determine whether there are precedents for a customer's problem and to facilitate finding reusable solutions to common INFOSEC problems.

5239-15* **Controlled Access Protection Guide**

Aids the user and security staff in understanding the DoN Controlled Access Protection policy, its relationship to C2, and techniques activities can use to acquire CAP compliant systems.

5239-16 **Risk Assessment Guidebook**

Provides policy and step-by-step procedures to individuals responsible for accomplishing a risk analysis on systems. Provides methods for the determination of system sensitivity and criticality, accomplishment of risk

assessment and economic analysis, and determination of environmental hazards and threats to DoN information systems.

5239-18 Security Test and Evaluation Guidebook

Provides information on how to perform security test and evaluation (ST&E) for information systems, embedded computers, and networks. It addresses microcomputers, minicomputers, mainframes, and specialized computers in both stand-alone and networked environments. The instruction provides general guidance and procedures to security managers and users for conducting ST&Es.

5239-19 Computer Incident Response Guidebook

Aids the, ISSM, ISSO, and users in responding to security incidents involving computer penetrations or malicious code. Provides general guidance for planning activity response and specific procedures for coordination with NAVCIRT.

5239-23 COMSEC Embedding Guidebook

Provides design guidelines for embedding INFOSEC modules .

5239-26* Remanence Security Guidebook

Provides policy, guidelines, and procedures for clearing and purging information systems memory and other storage media for release outside of and for reuse within controlled environments. It pertains to both classified and sensitive unclassified information. Implements DOD 5200.28-M and CSC-STD-005-85.

5239-29* Controls Over Copyrighted Computer Software

Assists DON activities in developing and implementing their own policies and procedures for controlling and using computer software programs having licensing agreements and copyright protection within the DON.

Appendix B
Security Policy Documentation

Central Intelligence Agency

DCI Directive 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)," Secret, July 1988.

DCI Directive 1/16 establishes long-term (year 2000) goals and near-term (year 1992) requirements intended to improve the security of U.S. intelligence processed in automated information systems (AISs), and networks with respect to its possible compromise (1) due to penetration by hostile intelligence services, (2) by otherwise legitimate users who gain access to data or processes for which they are not authorized or (3) as a result of inadequate security design, implementation, or operation. The directive also assigns policy execution roles and responsibilities, and establishes a procedural framework within which they are to be implemented.

Department of Defense

Department of Defense Instruction 5000.2 , "Defense Acquisition Management Policies and Procedures," 23 February 1991.

Department of Defense Instruction 5000.2 establishes an integrated framework for translating broadly stated mission needs into stable, affordable acquisition programs that meet the operational user's needs and can be sustained, given projected resource constraints. It also establishes a rigorous, event-oriented management process for acquiring quality products that emphasizes acquisition planning, improved communications with users, and aggressive risk management by both Government and industry.

Department of Defense Directive 5200.1 , "Information Security Program," 7 June 1986.

Department of Defense Directive 5200.1 reissues DoD 52001-R, "Information Security Program Regulation", updates policies and procedures of the DoD Information Security Program, implements DoD 5200.1-H, "Department of Defense Handbook for Writing Security Classification Guidance", delegates authority, and assigns responsibilities.

Department of Defense Regulation 5200.1-R , "Information Security Program Regulation, "Department of Defense, August 1982.

DoD Regulation 5200-1.R governs the DoD information security program. It establishes a system for the classification, downgrading, and declassification of classified and sensitive information. It further states the policies and procedure for safeguarding national security information from unauthorized disclosure.

Department of Defense Directive C-5200.5 , "Communication Security (COMSEC) (U), "Confidential, 21 April 1990.

Department of Defense Directive C-5200.5 presents the policy necessary to ensure the security and protection of telecommunications systems that transmit classified and sensitive information. This information is highly susceptible to interception, technical exploitation, the human intelligence (HUMINT) threat, and other dimensions of the foreign intelligence threat.

Department of Defense Directive C-5200.19*, "Control of Compromising Emanations (U), " Confidential, 23 February 1990.*

Department of Defense Directive 5200.28, "Security Requirements for Automated Information Systems, " Department of Defense, March 1988.

DoD Directive 5200.28 provides the mandatory, minimum AIS security requirements for processing classified, sensitive unclassified, and unclassified information. The directive states that information in AISs shall be safeguarded at all times by computer, communication, administrative, personnel, operations, emanations, and physical security measures. It stresses the importance of a life cycle management approach for implementing computer security requirements.

Department of Defense Directive 5200.28-STD , "Department of Defense Trusted Computer System Evaluation Criteria, "Department of Defense, December 1985.

DoD 5200.28-STD (also known as the "Orange Book" and "the Criteria") provides technical security requirements and evaluation methodologies for trusted computer systems. It provides a metric with which to evaluate the degree of trust that can be placed in a computer system. This standard also serves as a basis for specifying security requirements in computer system acquisition documentation.

Department of Defense Instruction 5215.2 , "Computer Security Technical Vulnerability Reporting Program (CSTVRP)," 2 September 1986.

Department of Defense Instruction 5215.2 establishes: 1) a Computer Security Technical Vulnerability Reporting Program (CSTVRP) under the direction of the National Security Agency, National Information Security Assessment Center (NISAC), 2) Procedures for reporting all demonstrable and repeatable technical vulnerabilities of Automated Information Systems (AIS), 3) Provides for the collection, consolidation, analysis, reporting or notification of generic technical vulnerabilities and corrective measures in support of the DoD Computer Security requirements and 4) Methodologies for dissemination of vulnerability information.

Military Standard 1785 , "System Security Program Management Requirements," 01 September 1989.

Military Standard 1785 establishes the formats, contents and procedures for a contract SSE Management Program. It also establishes definitive guidance in the initial acquisition or modification of new or existing systems, equipment, and facilities to analyze security design and engineering vulnerabilities; and develop recommendations for engineering changes to eliminate or mitigate vulnerabilities consistent with other design and operational considerations. SSE supports the development of programs and standards to provide life cycle security for critical defense resources.

Department of the Navy

SECNAVINST 5231.1C , "Life Cycle Management of Automated Information Systems within the Department of the Navy," 10 July 1992

SECNAVINST 5231.1C updates policy relative to Life Cycle Management (LCM) as the standard discipline for managing and obtaining approval for Information Systems (IS) projects as defined by DODD 7920.1 "Life Cycle Management of Automated Information Systems (NOTAL)," 20 June 1988 and DODI 7920, "Automated Information System Life Cycle Management Review and Milestone Approval Procedures (NOTAL)," 7 March 1990.

SECNAVINST 5239.2, "Department of the Navy Automated Information Systems Security Program," Department of the Navy, November 1989.

SECNAVINST 5239.2 established the DON AIS security program, defining the organizational structure and setting forth the policies and guidelines to implement the program. The objective of this instruction is to ensure the availability of reliable information and automated support by protecting AISs and networks from unauthorized disclosure, accidental or intentional destruction, unauthorized modification, and denial of service conditions.

OPNAVINST 5239.1A, "Department of the Navy Automated Data Processing Security Program, " Department of the Navy, August 1982.

OPNAVINST 5239.1A consolidates Navy policies on the security evaluation of AISs. The instruction delineated the requirements and assigns roles and responsibilities for accreditation of AISs. It provides guidance for the risk assessment process and full accreditation requirements.

Marine Corps Order P5510.14 , "Marine Corps Automatic Data Processing (ADP) Security Manual," 2 January 1981.

Marine Corps Order P5510.14 provides centralized guidance and uniform policy on all known and recognized aspects of Automatic Data Processing (ADP) security. It also provides realistic guidance and generalized procedures to ensure that all sensitive defense information handled by automated systems is protected against espionage, sabotage, fraud, misappropriation, misuse, or inadvertent or deliberate compromise.

Marine Corps Order 5271.1 , “Information Resources management (IRM) Standards and Guidelines Program, 10 June 1993.

Marine Corps order 5271.1 establishes the IRM Standards and Guidelines Program and authorizes the development and distribution of publications. The IRM Program is the primary means through which technical direction is exercised. The program is designed to facilitate the rapid publication of standards and guidelines covering all aspects of the management of information resources, including INFOSEC.

SECNAV 5200.32A , "Acquisition Management Policies and Procedures for Computer Resources,", 03 May 1993.

SECNAV 5200.32A provides policy for acquiring Department of the Navy (DON) computer resources and to establish the internal management processes. It authorizes the promulgation of the Open System Interface Standards List (OSISL) and the Products Accepted List (PAL) in SECNAVNOTE 5200, Subj: Acquisition Management Policies and Procedures for Computer Resources, to facilitate the acquisition of computer resources in accordance with this instruction.

Executive Office/Congress and National Branch

Executive Order 12356 , "National Security Information," 2 April 1982.

Executive Order (EO) 12356 established a system for classifying , declassifying, and safeguarding national security information. It identifies classification authorities and describes their general responsibilities for the origination and handling of classified information.

National Security Decision 42 , "National Policy for the Security of National Security Telecommunications and Information Systems," Executive Office of the President, July 1990.

National Security Decision 42 establishes initial objectives, policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; established a mechanism for policy development and dissemination; and assigned responsibilities for implementation.

National Telecommunications and Information Systems Security Policy No. 200 , "National Policy on Controlled Access Protection, "National Telecommunications and Information Systems Security Committee, July 1987.

Under the authority of NSDD 145, National Telecommunications and Information Systems Security Policy (NTISSP) No. 200 defines the minimum level of protection for AISs

processing classified or sensitive unclassified information. It prescribes the C2 class criteria of DoD 5200.28-STD as the minimum level of protection for such systems, with additional protection required if warranted by a system risk assessment.

Public Law 100-235 , "Computer Security Act of 1987," 8 January 1988.

Public Law 100-235 redefines the role of the National Institute of Standards and Technology (formerly the National Bureau of Standards) and establishes a new Computer System Security and Privacy Advisory Board. It requires each federal agency to 1) Provide for mandatory periodic training in computer security awareness and accepted computer security practices, 2) Identify each federal computer system and system under development which contains sensitive information and 3) Establish a plan for security and privacy of such systems.

Joint Staff

Chairman of the Joint Chiefs of Staff Instruction CJCSI 6510.01 , "Joint and Combined Communications Security," 1 September 1993.

Chairman of the Joint Chiefs of Staff Instruction CJCSI 6510.01 establishes policy and procedures for planning and conducting joint and combined COMSEC. Applicable policy to joint and combined applications was presented: Transmission of Sensitive Information, System Planning, Operational Planning, Joint Coordination, Urgent Need, Foreign Release, Foreign Sales, Radios, Special-Purpose Cryptoequipment, Manual Systems Cryptonet Size, Cryptoperiod, Radio Frequencies, Call Signs, Field Generation and Over-The Air Distribution (OTAD) of Tactical Key, Intertheater COMSEC Package Key, Assessments, COMSEC Monitoring and TEMPEST.

JCS Memorandum MJCS-38-89 , "Use of Standard Embedded Cryptography," 2 March 1989.

JCS Memorandum MJCS-38-89 encourages maximum use of standard embedded cryptography products in future communications and computer systems that require cryptographic security features.

National Computer Security Center

CSC-STD-002-85 , "Department of Defense Password Management Guideline," 12 April 1985.

CSC-STD-002-85 assists in providing credibility of user identity by presenting a set of good practices related to the design, implementation and use of password-based user authentication mechanisms. It is intended that the features and practices described in the guideline be incorporated into DoD automatic data processing (ADP) systems for processing classified or other sensitive information.

CSC-STD-003-85, "Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in specific Environments," National Computer Security Center, June 1985.

This document provides guidance for specifying computer security requirements for the DoD by identifying the minimum class of system required for a given risk index.

CSC-STD-004-85, "Technical Rationale Behind CSC-STD-003085: Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in specific Environments," National Computer Security Center, June 1985.

This document provides background discussion and rationale for CSC-STD-003-85, and provides additional and more detailed guidance for specifying computer security requirements for the DoD by identifying the minimum class of system required for a given risk index for different environments.

CSC-STD-005, Department of Defense Magnetic Remanence Security Guideline," 15 November 1985.

CSC-STD-005 provides procedures and guidelines for declassifying and clearing Automatic Data Processing (ADP) magnetic memory and other ADP magnetic storage media.

NCSC-TG-005, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, "National Computer Security Center, Version 1 July 1987.

The Trusted Network Interpretation (TNI or "Red" Book") was issued by the National Computer Security Center (NCSC) as part of its program to promulgate technical computer security guidelines. The interpretation extends the evaluation classes of the "Orange Book" to trusted network systems and components.

National Institute of Standards and Technology

Federal Information Processing Standard on Trusted Systems Technology , "Minimum Security Functionality Requirements for Multi-User Operating Systems, Issue 1, 16 January 1992.

The Minimum Security Requirements for Multi-User Operating Systems (MSR) document provides basic commercial computer system security requirements applicable to both government and commercial organizations. These requirements include technical measures that can be incorporated into multi-user, remote-access, resource-sharing, and information-sharing computer systems.

Federal Information Processing Standard on Trusted Systems Technology , "Federal Criteria for Information Technology Security, Protection Profile Development," Volume 1, Version 1.0, December 1992.

The Federal Criteria for Information Technology Security, Protection Profile Development Volume 1, Version 1.0 provides a basis for developing, analyzing, and registering criteria for information technology (IT) product security development and evaluation. It explains how to use provided generic requirements as building blocks to create unique sets of IT product security criteria called protection profiles. There are four principal objectives: 1) Develop an extensible and flexible framework for defining new requirements for IT product security, 2) Enhance existing IT product security development and evaluation criteria, 3) Facilitate international harmonization of IT product security development and evaluation criteria and 4) Preserve the fundamental principles of IT product security.

National Security Telecommunications and Information Systems Security Committee

NTISSD 500, "Information Systems Security (INFOSEC) Education, Training, and Awareness," 25 February 1993.

NTISSD 500 establishes the requirement for federal departments and agencies to develop and/or implement Telecommunications and Automated Information Systems Security (TAISS) education and training programs and TAISS awareness activities.

NTISSD 501, "National Training Program for Information Systems Security (INFOSEC) Professionals," 16 November 1992.

NTISSD 501 establishes the requirement for federal departments and agencies to implement training programs for information systems security (INFOSEC) professionals. For the purpose of the directive, an INFOSEC professional is an individual who is responsible for the security oversight or management of national security systems during each phase of the life cycle.

NTISSD 502, "National Security Telecommunications and Automated Information Systems Security," 5 February 1993.

NTISSD 502 delineates and clarifies objectives, policies, procedures, standards and terminology as set forth in the "National Policy for the Security of National Security Telecommunications and Information Systems," (National Security Decision 42) dated July 1990. The National Security Decision 42 established the initial national objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding, from exploitation, systems that process or communicate national security information, established a mechanism for policy development, and assigned responsibilities for implementation.

National Security Decision 42 establishes initial objectives, policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; established a mechanism for policy development and dissemination; and assigned responsibilities for implementation.

NTISSP 4, "National Policy on Electronic Keying," 16 November 1992.

NTISSP 4 declares that all U.S. Government departments and agencies shall establish and implement electronic keying programs with the objective of virtually eliminating, by the year 2000, their dependence on paper-based/non-electronic keying methods and with a goal of implementing benign keying where appropriate. Electronic keying shall be applied to all cryptographic processes related to national security systems. U.S. Government departments and agencies shall exchange electronic keying information freely, coordinate programs, and participate in consolidated programs wherever possible.

NTISSP 200, "National Policy on Controlled Access Protection," 15 July 1987.

NTISSP 200 states that all automated information systems which are accessed by more than one user, when those users do not have the same authorization to use all of the classified or sensitive unclassified information processed or maintained by the automated information system, shall provide automated Controlled Access Protection for all classified and sensitive unclassified information.

Office of Management and Budget

Office of Management and Budget Circular A-130 , "Management of Federal Information Resources," Executive Office of the President, December 1985.

Office of Management and Budget (OMB) Circular A-130 establishes general policy for the management of Federal information resources. Included in this circular is policy for the security of Federal AISs. The circular establishes minimum controls for inclusion in AIS security programs and assigns responsibilities for the security of AISs.

Space and Naval Warfare Systems Command

"Computer Security Guidebook for Mission-Critical Computer Resources Managed under the Research, Development, and Acquisition Process" , Space and Naval Warfare Systems Command Engineering Policy Division (SPAWAR 321), October 1990.

"Computer Security Guidebook for Mission-Critical Computer Resources Managed under the Research, Development, and Acquisition Process" provides detailed interim guidance to Navy program managers on how to address computer security requirements during the acquisition process.

Appendix C

Acronym List

C^4I	Command, Control, Computers, Communications, and Intelligence
COMPUSEC	Computer Security
COMSEC	Communications Security
DAA	Designated Approval Authority
DII	Defense Information Infrastructure
DoN	Department of the Navy
IATO	Interim Authority to Operate
INFOSEC	Information System Security
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
NAVSO P	Naval Staff Office Publication
NII	National Information Infrastructure
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
ST&E	Security Test and Evaluation
TASO	Terminal Area Security Officer